Frequency Rendezvous for Fast and Resilient Key Establishment under Jamming Attack

Eun-Kyu Lee, Soon Y. Oh, and Mario Gerla
Computer Science Department
University of California, Los Angeles
Los Angeles, CA, USA
{eklee, soonoh, gerla}@cs.ucla.edu

Abstract—Jamming attacks have been recently studied as wireless security threats disrupting reliable RF communication in a wireless network. Recently, spread spectrum techniques have been proposed as promising countermeasures to avoid the jamming attacks. However, these solutions require a secure pre-key establishment phase before data transmission, which takes considerable time and thus provides limited functionality. In order to solve the problem, this paper proposes a novel Frequency Quorum Rendezvous (FQR) scheme. Nodes hop over random frequencies independently during the phase, supporting anti-jamming communications. By using a quorum system, nodes are guaranteed to meet, which could reduce time latency. We validate the proposed scheme via extensive simulations.

I. INTRODUCTION

The shared wireless medium makes wireless communications vulnerable to jamming attacks, in which an adversary (jammer) intentionally injects noise-like signals into the wireless network. Recently, spread spectrum techniques such as Frequency Hopping Spread Spectrum (FHSS) have been intensively investigated as countermeasures against jamming attacks. Communication parties rely on a pre-shared common key (hopping sequence) which is unknown to the jammer, thus making the system robust against jamming attacks. This, however, raises another issue of how to exchange the key securely under jamming attacks, namely key establishment phase. To solve the problem, recent approaches [4, 5] adopt a Pseudo-random Frequency Hopping (PFH) technique from Bluetooth. During a key establishment phase, nodes in PFH randomly hop over multiple frequencies. Upon meeting on the same frequency by chance, they exchange the common key. Relying on random encounters among nodes causes serious time cost to complete the phase. In the worst case, it could take up to 100 seconds [1, 5], which is unacceptable in tactical or emergency scenarios where time sensitive information must be exchanged.

In this work, we propose a Frequency Quorum Rendezvous (FQR) scheme for resilient and fast key establishment. FQR exploits a quorum system which allows each node to build a hopping sequence independently during the key establishment phase; thus it achieves robust communication. The concept of guaranteed rendezvous of the quorum system ensures a pair of nodes to meet within a specified time, which reduces time latency of the phase. In addition to described benefits, we want to note that this is the first work that uses quorum for rendezvous in a hostile, jamming environment.

The rest of the paper is organized as follows. Section II presents the proposed FQR scheme in detail. In Section III, we evaluate FQR with simulation results. Finally, we conclude the paper in Section IV.

II. FREQUENCY QUORUM RENDEZVOUS

A. Quorum System

A quorum system is as a collection of subsets of a given universal set, in which any pair of two subsets (quorums) have at least one element in common [3]. The proposed FQR scheme exploits a cyclic quorum system [2] to construct a set of hopping sequences. This subsection gives a brief description on it.

DEFINITION 1. A subset \( D = \{a_1, ..., a_\kappa\} \subset \mathbb{Z}_N \), \( a_i \in \{0, ..., N - 1\} \) and \( \kappa \leq N \), is called a cyclic \((N, \kappa)\) difference set if for every \( d \neq 0 \pmod{N} \) there exist at least one pair of elements \((a_i, a_j)\) such that \( a_i - a_j \equiv d \pmod{N} \).

DEFINITION 2. Given a \((N, \kappa)\) difference set \( D = \{a_1, ..., a_\kappa\} \subset \mathbb{Z}_N \), a cyclic quorum system constructed by \( D \) is \( Q = \{G_0, ..., G_{N-1}\} \), where \( G_i = \{a_1 + i, a_2 + i, ..., a_\kappa + i\} \pmod{N} \) and \( i = 0, ..., N - 1 \).

B. Frequency Quorum Rendezvous

A frequency hopping system is constructed by assigning frequencies to \( t \) time slots and determining a frequency hopping sequence in one period, \( X \):

\[ X = \{x_0, ..., x_t\} = \{(0, c_0), ..., (t - 1, c_{t-1})\}, \]

where \( x_i \in X \) contains a tuple of \((time\ slot\ index,\ frequency\ index)\) and \( c_i \in \{0, ..., N - 1\} \) represents the frequency index at time slot \( i \) in a time period. Given two frequency hopping sequences \( X \) and \( Y \), they are said to rendezvous if they have...
at least one element in common: \( x_i = y_i \) \((0 \leq i \leq t - 1)\). If a pair of nodes selects the rendezvous sequences of \( X \) and \( Y \) respectively, then they are guaranteed to be on the same frequency at the same time at least once within a period.

By applying the cyclic quorum system, the proposed FQR system is constructed by assigning frequencies to time slots. We present our algorithm with an example by setting \( N = 7 \) and \( \kappa = 3 \) as follows.

1) Construct a universal set \( U = \mathbb{Z}_7 = \{0, ..., 6\} \) and determine a \((7,3)\) difference set \( D, (\sqrt{7} \leq 3 \leq 7). \)
2) Construct a cyclic quorum system \( Q = \{G_0, ..., G_6\} \) from \( D \).
3) A node \( A \) selects a random number \( 5 \) from \( U \), and then obtains a quorum \( G_5 = \{5, 6, 1\} \) from \( Q \).
4) The following equation assigns a frequency to the time slot \( j \) using the quorum \( G_5 = \{g_0, g_1, g_2\} = \{5, 6, 1\} \).
   \[ x_j = (j, g_m) \text{ and } y_j = (j, g_n) \]
   where \( m = j \mod \kappa \) and \( n = (j - (j \mod \kappa)) / \kappa \).
5) Repeat step (4) for all \( 9 = \kappa^2 \) time slots. This constructs a sending sequence \( X = \{(0, 5), (1, 6), (2, 1), (3, 5), (4, 6), (5, 1), (6, 5), (7, 6), (8, 1)\} \) and a receiving sequence \( Y = \{(0, 5), (1, 5), (2, 5), (3, 6), (4, 6), (5, 6), (6, 1), (7, 1), (8, 1)\} \)
6) A node \( B \) repeats step (4-5) with a selected quorum \( G_3 = \{3, 4, 6\} \), and then, construct two hopping sequences \( X' \) and \( Y' \).

Figure 1 illustrates rendezvous at the FQR system when the nodes \( A \) and \( B \) choose the sequence \( X \) and \( Y' \), respectively. As shown, they rendezvous on channel 6 at time slot 7.

### III. Simulations and Results

In Figure 2(a), FQR shows a lower latency than those of PFH and RH, which indicates that a sender rendezvous with a receiver quickly. The gaps become clear as \( N \) increases because nodes in RH or PFH randomly select frequencies. A low RFC value in Figure 2(b) indicates that more frequencies are used for rendezvous; thus a jammer can hardly launch an efficient attack. PFH presents the worst performance. As a receiver sits on one frequency for 20 time slots regardless of \( N \) values, rendezvous is limited only to the frequency, which degrades the RFC performance. FQR works better than RH since it takes \( \kappa \) adaptively along with increasing \( N \).

### IV. Conclusion

We have presented a novel Frequency Quorum Rendezvous (FQR) scheme that achieves fast and resilient key establishment, making wireless communication more robust against jamming attacks. FQR allows nodes to hop over multiple frequencies based on sequences selected individually and randomly. Thus, communication is robust against jamming attacks. In addition, the quorum system guarantees that the nodes meet within a bounded time, which decreases time overhead for the key establishment. The experimental results showed that the proposed scheme outperforms existing methods. For further work, we will examine FQR with more various jamming attack models and enhance it to develop a robust multicast protocol.

### References


